Matrix E1
(1G582-09 and 1H582-51)
WebView User's Guide

9033782

ENTERASYS NETWORKS™

NOTICE

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.
35 Industrial Way
Rochester, NH 03866-5005

Order Number: 9033782 February 2002

Version:	Information in this guide refers to Matrix E1 1G582-09 and 1H582-51 firmware version 1.00.xx.

ENTERASYS NETWORKS, INC.
PROGRAM LICENSE AGREEMENT

BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.

This document is an agreement ("Agreement") between You, the end user, and Enterasys Networks, Inc. ("Enterasys") that sets forth your rights and obligations with respect to the Enterasys software program ("Program") in the package. The Program may be contained in firmware, chips or other media. UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS (603) 332-9400. Attn: Legal Department.

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Enterasys.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

4. EXPORT REQUIREMENTS. You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the product is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The enclosed Product (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Product is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

6. EXCLUSION OF WARRANTY. Except as may be specifically provided by Enterasys in writing, Enterasys makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

ENTERASYS DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY ENTERASYS IN WRITING, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

7. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS ENTERASYS PRODUCT, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR IN THE DURATION OR LIMITATION OF IMPLIED WARRANTIES IN SOME INSTANCES, THE ABOVE LIMITATION AND EXCLUSIONS MAY NOT APPLY TO YOU.

Contents

Figures

Tables

About This Guide

Welcome to the Enterasys Networks ***Matrix E1 (1G582-09 and 1H582-51) WebView User's Guide***. This manual explains how to perform Local Management tasks on the Matrix E1 1G582-09 and 1H582-51 devices using WebView. Enterasys Networks' HTTP-based Web management application, WebView is an intuitive tool for initial configuration and simple management tasks.

Important Notice

Depending on the firmware version used in the Matrix E1 device, some features described in this document may not be supported. Refer to the Release Notes shipped with the Matrix E1 device to determine which features are supported.

USING THIS GUIDE

A general working knowledge of basic network operations is helpful before configuring the Matrix E1 device.

This manual describes how to do the following:

- Access the Matrix E1 WebView application.
- Navigate through Matrix E1 WebView screens.
- Use the screens to perform initial device configuration and simple network management tasks.

STRUCTURE OF THIS GUIDE

The guide is organized as follows:

Chapter 1, **Introduction**, provides an introduction to WebView, an overview of the Matrix E1 Local Management tasks that may be accomplished using WebView, and information on how to contact Enterasys Networks for technical support.

Chapter 2, **Starting and Navigating WebView**, provides information about preparing to use WebView, starting the WebView application, WebView security features, an overview of the WebView user interface, how to navigate through WebView screens, and describes port designations in WebView.

Chapter 3, **WebView Local Management Tasks**, provides information about using WebView screens to perform Local Management tasks, such as viewing and configuring device settings, configuring IP settings, configuring SNMP traps and community names, downloading a new firmware image via TFTP server, adding new static MAC and VLAN addresses to the device's address table, viewing and configuring Spanning Tree device and per-port settings, and configuring the device's VLAN, port and port priority settings.

RELATED DOCUMENTS

The following Enterasys Networks documents may help you to set up, control, and manage the Matrix E1 device:

- *Ethernet Technology Guide*
- *Cabling Guide*
- *Matrix E1 (1G582-09 or 1H582-51) Installation Guide*
- *Matrix E1 (1G582-09 and 1H582-51) Configuration Guide*

Documents listed above, can be obtained from the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following web site:

http://www.enterasys.com/

DOCUMENT CONVENTION

This guide uses the following convention:

NOTE: Calls the reader's attention to any item of information that may be of special importance.

TYPOGRAPHICAL CONVENTIONS

bold type	Bold type denotes user input, field names, and valid field entries.
italic type	Italic type indicates complete document titles.
ENTER	Indicates either the ENTER or RETURN key, depending on your keyboard.

1

Introduction

This chapter provides an introduction to WebView, an overview of the Matrix E1 1G582-09 and 1H582-51 Local Management tasks that can be accomplished using WebView, and information on how to contact Enterasys Networks for technical support.

Important Notices

Depending on the firmware version used in the Matrix E1 1G582-09 or 1H582-51 device, some features described in this document may not be supported. Refer to the Release Notes shipped with the Matrix E1 device to determine which features are supported.

This guide is intended to supplement the *Matrix E1 (1G582-09 and 1H582-51) Configuration Guide*, which details the devices' Command Line Interface (CLI) commands and how they are used. Since CLI is the primary interface for managing and configuring the Matrix E1, the Configuration Guide will guide you in performing the devices' full set of switch management configurations.

1.1 ABOUT WEBVIEW

Enterasys Networks' embedded Web server, WebView, provides World Wide Web (WWW) browser access to Enterasys hardware. The server is built into the Matrix E1 firmware and provides basic management and simple configuration for the device. With this tool, managers are able to manage WebView-compliant hardware from any Web-accessible location. WebView provides network managers with a convenient way to perform basic configuration, maintenance and troubleshooting through the WWW interface. Access to Local Management via WebView is as simple as opening a URL in a web browser to the IP address of the Matrix E1 device. WebView supports Netscape Navigator and Microsoft Internet Explorer with JDK 1.1 support.

1.2 USING WEBVIEW WITH MATRIX E1 DEVICES

WebView is an intuitive tool for initial configuration and simple management tasks. It allows a network manager to perform the following tasks:

- Assign a new IP address and subnet mask to the device.
- Select a default gateway.
- Assign a login password to the device for additional security.
- Download a new firmware image.
- Designate which network management workstations receive SNMP traps from the device.
- View device and RMON statistics.
- Enable ports to operate in standard or full duplex mode.
- Configure ports to perform load sharing using trunking commands.
- Set flow control on a port-by-port basis.
- Configure ports to prioritize incoming frames.
- Set 802.1Q VLAN memberships.
- View and configure basic Spanning Tree device and per-port settings.

1.3 GETTING HELP

For additional support related to this device or document, contact Enterasys Networks using one of the following methods:

World Wide Web	http://www.enterasys.com/
Phone	(603) 332-9400
Internet mail	support@enterasys.com
FTP	ftp://ftp.enterasys.com/
Login	*anonymous*
Password	*your email address*

To send comments or suggestions concerning this document, contact the Enterasys Networks Technical Writing Department via the following email address: **TechWriting@enterasys.com**

Make sure to include the document Part Number in the email message.

Before calling Enterasys Networks for technical support, have the following information ready:

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

2

Starting and Navigating WebView

This chapter provides information about the following:

- Preparing to use WebView (Section 2.1)
- Starting WebView (Section 2.2)
- WebView security (Section 2.3)
- Overview of the WebView user interface (Section 2.4)
- Navigating through WebView screens (Section 2.5)
- Port designations in WebView (Section 2.6)

2.1 PREPARING TO USE WEBVIEW

Before you can use WebView for Matrix E1 Local Management, you must:

1. Set up the device and connect a console port, as described in the *Matrix E1 (1G582-09 and 1H582-51) Installation Guide.*
2. Access the Command Line Interface (CLI) and use the CLI **set IP** command to configure an IP address for the device as described in the *Matrix E1 (1G582-09 and 1H582-51) Configuration Guide.*
3. If necessary, enable WebView and set the WebView port.

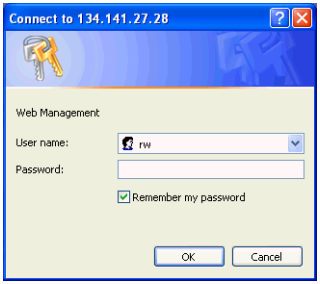
NOTE: By default, WebView is enabled on the device and set to run through TCP port 80. If these settings have been changed, you may need to re-enable WebView using the CLI **set webview enable** command, and reset the port using the **set webview port** command. For details, refer to the Configuration Guide.

2.2 STARTING WEBVIEW

To start a WebView session:

1. Open Microsoft Internet Explorer or Netscape Navigator.
2. In the address URL field, type the IP address of the WebView-enabled device you wish to access and press ENTER. The WebView Web Management login security screen, Figure 2-1, displays. (For details on WebView security, refer to Section 2.3).

Figure 2-1 WebView Web Management Login Security Screen



3. Enter **rw** for **User name**.
4. Leave the **Password** field blank. Press ENTER. The WebView user interface Figure 2-2, displays.

2.3 WEBVIEW SECURITY

WebView security is administered with the use of SNMP community name strings and is limited to two access levels:

- Read-Only: Allows users to view appropriate content available in WebView, but does not allow them to modify any information.
- Read-Write: Allows users access to full administrative privileges.

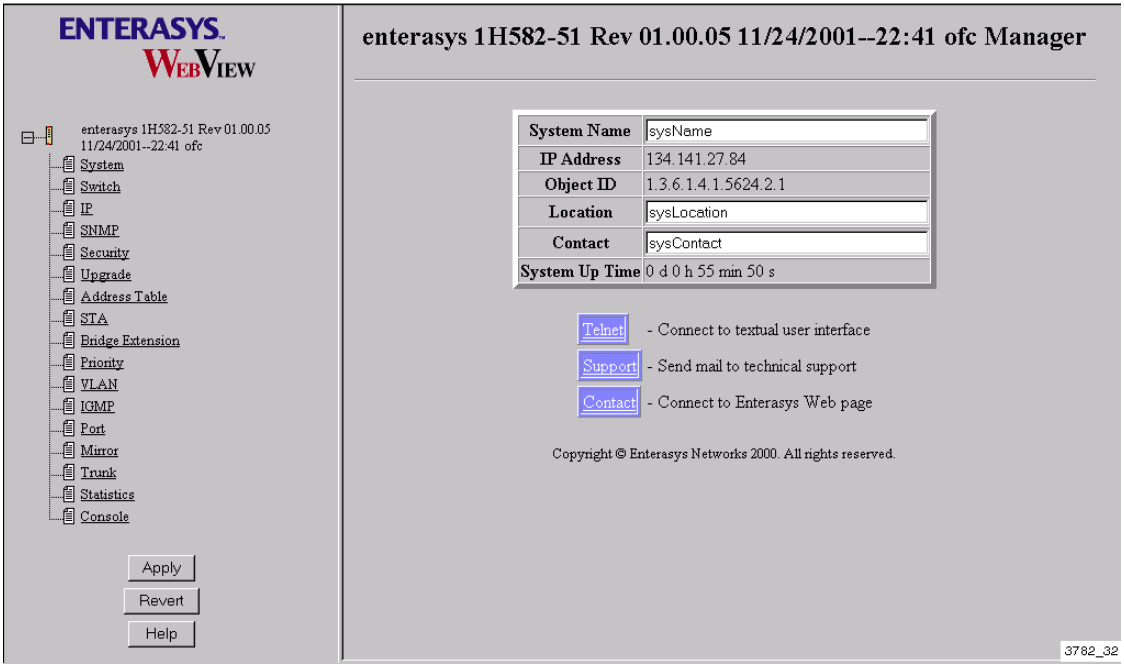
After the user enters the appropriate URL, the WebView server prompts for a **User name** and **Password**. Appropriate entries on this login screen allow access to the WebView device.

NOTE: By default, the **User name** is set up for Read-Write (**rw**) access. This permits read-write access to all modifiable parameters. The default password is set to blank. For information on setting a new **Password**, refer to Section 3.7.

2.4 OVERVIEW OF THE WEBVIEW USER INTERFACE

As shown in Figure 2-2, the WebView user interface (UI) is a traditional frames presentation consisting of a navigation frame on the left side of the screen, and a content frame on the right side of the screen. The navigation frame allows you to select the available Matrix E1 information and configuration functions. Screens in the content frame display the function selected from the navigation frame.

Figure 2-2 WebView User Interface



2.5 NAVIGATING WEBVIEW

The WebView navigation frame displays a list of links that enable you to go to a particular screen by selecting its function from the list. The navigation frame also displays buttons allowing you to **Apply** the changes made in a content screen; **Revert** to previous configuration settings, and go to

WebView online **Help**. Table 2-1 describes the screen links in the navigation frame and their functions.

Table 2-1 Screen Designations and Functions in the Navigation Frame

Click on...	To...
System	Go to the System screen, where you can view and configure system (device) settings, such as the name and location of the device. Links on this screen also enable you to Telnet to the textual Command Line Interface (CLI), to send email to Enterasys technical support, and to connect to the Enterasys Web page.
Switch	Go to the Switch Information screen, where you can view information about the main system board, including serial number, number of ports, and hardware and firmware versions.
IP	Go to the IP Configuration screen, where you can set the host IP state, IP address, subnet mask, gateway IP address, and maximum number of Telnet sessions allowed, and view the device's MAC address.
SNMP	Go to the SNMP Traps Configuration and SNMP Community Names screens. Here you can assign IP addresses where SNMP traps will be sent, enable or disable traps, and set SNMP community names and access policies associated with these traps.
Security	Go to the Security Configuration screen, where you can set a new login password for the device.
Upgrade	Go to the TFTP Download Management screen, where you can download a new firmware image from a TFTP server to the device.
Address Table	Go to the Address Table Configuration screen, where you can view entries in the device's address table, add new static address entries, remove entries, and view counts of dynamic and static addresses in the address table.

Table 2-1 Screen Designations and Functions in the Navigation Frame (Continued)

Click on...	To...
STA	Go to the STA Information, STA Configuration, and STA Port Configuration screens, where you can view and configure STA (Spanning Tree Algorithm) settings for the device and for individual ports.
Bridge Extension	Go to the Bridge Extension Configuration screen, where you can view bridge MIB extension capabilities configured on the device, and set the host VLAN ID.
Priority	Go to the Port Priority Configuration and Port Traffic Class Information screens, where you can set the default ingress port priority per port, view the number of egress traffic classes per port, and view port priority-to-transmit queue mapping information.
VLAN	Go to the VLAN Basic Information, VLAN Current Table, VLAN Static List, VLAN Static Table, VLAN Static Membership by Port, and VLAN Port Configuration screens. Here you can view basic information about the numbers of VLANs configured and about all static and dynamically created VLANs known to the device, create new or remove existing static VLANs from the device, configure a static VLAN's egress list, add ports to or remove ports from a static VLAN, assign default VLAN IDs to untagged frames, and enable or disable ingress filtering on one or more ports.
IGMP	Go to the IGMP Configuration and the IP Multicast Registration Table screens, where you can enable IGMP (Internet Group Management Protocol) on the device, configure IGMP parameters, and view the status of IGMP groups.
Port	Go to the Port Information and Port Configuration screens, where you can view and set port administrative, link, speed, duplex and flow control status.

Table 2-1 Screen Designations and Functions in the Navigation Frame (Continued)

Click on...	To...
Mirror	Go to the Mirror Port Configuration screen, where you can enable port mirroring on the device and set a source and target port for mirroring.
Trunk	Go to the Port Trunking Configuration screen, where you can add or remove trunks on the device, and add or remove trunk ports from existing trunks.
Statistics	Go to the Port Statistics screen, where you can view port Ethernet-like MIB statistics and RMON statistics.
Console	Go to the Console Configuration screen, where you can configure device console settings, such as baud rate, time out, and auto refresh rate.
Apply	Apply entries made to the WebView screen on display.
Revert	Clear entries made to the WebView screen on display.
Help	Go to WebView online help for this Matrix E1 device.

2.6 PORT DESIGNATIONS IN WEBVIEW

The expansion module and fixed front panel port numbering scheme used when configuring Matrix E1 ports is shown in Figure 2-3. Fixed front panel ports 1 through 48 are RJ45 10/100 Ethernet connections. In WebView screens with **Port** listings, these fixed front panel ports are designated as 1 through 48.

The device's optional expansion module slots (1, 2, and 3), can have two to 16 ports depending on the module installed. Figure 2-4 shows the Ethernet Expansion Modules available at the time of this printing, and the location of the next consecutive port on each module. Table 2-2 shows the

numbering scheme for the fixed front panel, and for each expansion module installed in various slots, as it would appear in WebView screens with **Port** listings.

NOTE: The WebView port numbering scheme is based on the fact that each optional expansion module can have up to 16 ports. Therefore, designations for expansion modules with only two ports span all 16 numbers in the numbering sequence to allow for the possibility that the 2-port module could be exchanged with a 16-port module.

For information on how this device's port assignment scheme is expressed in CLI syntax, and considerations necessary for configuring port mirroring and trunking, refer to your *Matrix E1 Configuration Guide*.

Figure 2-3 Expansion Module and Fixed Front Panel Port Numbering Scheme

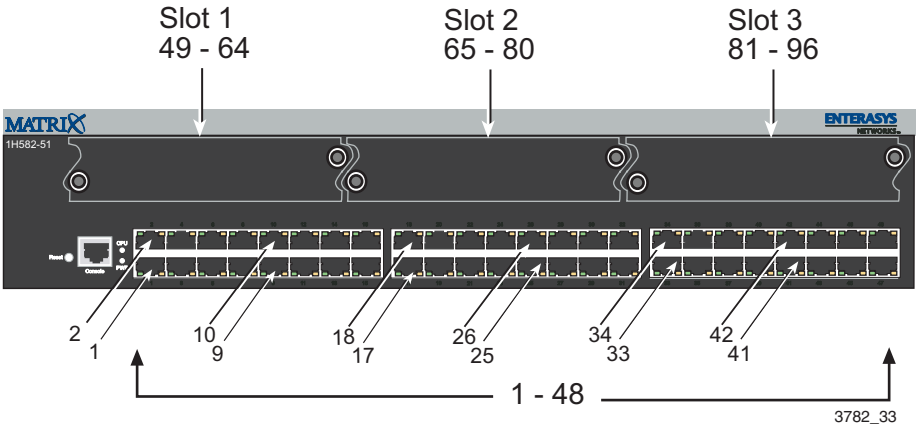


Figure 2-4 Sample Consecutive Port Numbering for Optional Expansion Modules

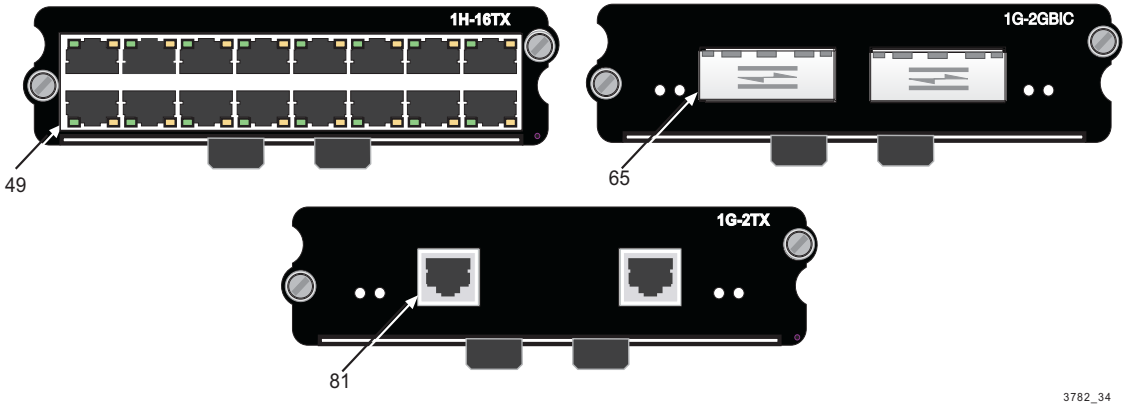


Table 2-2 Port Numbering Scheme with Expansion Modules Installed

Port/Module Type	Slot Location	Port Numbering Sequence
Fixed Front Panel Forty-eight fixed RJ45 ports Fast Ethernet 10/100BASE-TX	Front panel	| 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 | | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | | 33 | 35 | 37 | 39 | 41 | 43 | 45 | 47 | | 34 | 36 | 38 | 40 | 42 | 44 | 46 | 48 |
1H-16TX Expansion Module Sixteen fixed RJ45 ports Fast Ethernet 10/100BASE-TX	Installed in **Slot 1**	| 49 | 51 | 53 | 55 | 57 | 59 | 61 | 63 | | 50 | 52 | 54 | 56 | 58 | 60 | 62 | 64 |
	Installed in **Slot 2**	| 65 | 67 | 69 | 71 | 73 | 75 | 77 | 79 | | 66 | 68 | 70 | 72 | 74 | 76 | 78 | 80 |
	Installed in **Slot 3**	| 81 | 83 | 85 | 87 | 89 | 91 | 93 | 95 | | 82 | 84 | 86 | 88 | 90 | 92 | 94 | 96 |
1G-2TX Expansion Module Two fixed RJ45 ports Fast Ethernet 1000BASE-TX	Installed in **Slot 1**	| 49 | 57 |
	Installed in **Slot 2**	| 65 | 73 |
	Installed in **Slot 3**	| 81 | 89 |
1G-2GBIC Expansion Module Two port slots for optional GBICs Gigabit 1000BASE-SX/LX	Installed in **Slot 1**	| 49 | 57 |
	Installed in **Slot 2**	| 65 | 73 |
	Installed in **Slot 3**	| 81 | 89 |

3

WebView Local Management Tasks

3.1 OVERVIEW

This chapter provides information about using WebView screens to perform the following Local Management tasks:

- Viewing and configuring device settings, such as the device name and location of the device (Section 3.2).
- Viewing switch information, such as number of ports and the device's firmware version (Section 3.3).
- Configuring IP settings, such as the device's IP address, MAC address and maximum number of Telnet sessions allowed (Section 3.4).
- Configuring SNMP traps (Section 3.5) and community names (Section 3.6).
- Setting a new password for the device (Section 3.7).
- Downloading a new firmware image from a TFTP server (Section 3.8).
- Adding new static MAC and VLAN addresses and viewing the device's address table (Section 3.9).
- Viewing and configuring Spanning Tree device and per-port settings (Section 3.10 through Section 3.12).
- Viewing the device's bridge extension settings (Section 3.13).
- Configuring the device's port priority settings (Section 3.14) and viewing port traffic class information (Section 3.15).
- Configuring VLAN settings, such as the device's current VLAN egress table, creating static VLANs, configuring the static VLAN table and the static VLAN membership by port, and setting port VLAN IDs (PVIDs) and ingress filtering (Section 3.16 through Section 3.21).
- Configuring IGMP settings, such as query count, report delay and the IP Multicast Registration Table (Section 3.22 and Section 3.23).

- Viewing and configuring port settings, such as administrative status (enabled or disabled), link, speed, duplex and flow control status, and configuring port mirroring and trunking (Section 3.24 through Section 3.27).
- Viewing port Ethernet-like statistics, such as transmission errors, and RMON statistics (Section 3.28).
- Configuring console settings, such as baudrate, time-out and auto-refresh time (Section 3.29).

3.2 SYSTEM SCREEN

When to Use

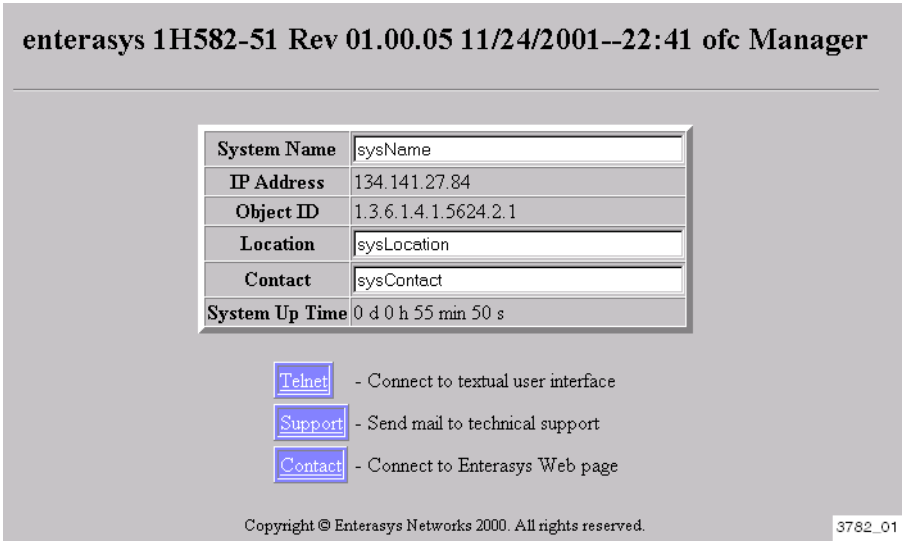
To view and configure system (device) settings, such as the name and location of the device. Links on this screen also enable you to Telnet to the textual Command Line Interface (CLI), to send email to Enterasys technical support, and to connect to the Enterasys Web page.

How to Access

Click on **System** in the WebView navigation frame. The System screen, Figure 3-1, displays.

Screen Example

Figure 3-1 System Screen



Screen Element Descriptions

Refer to Table 3-1 for a functional description of each screen field and link.

Table 3-1 System Screen Field and Link Descriptions

Use this field or link...	To...
System Name	See a name identifying the device or enter a new name. The default is **sysName**. Note that a name string containing a space in the text must be enclosed in quotes. For example: **"Information Systems"**.
IP Address	See the local host IP address.
Object ID	See the MIB II object identifier for the device's network management subsystem.
Location	See a name identifying the device location or enter a new location name. The default is **sysLocation**. Note that a name string containing a space in the text must be enclosed in quotes. For example: **"Bldg N32 Closet 9"**.
Contact	See a name identifying the contact person for the device or enter a new contact name. The default is **sysContact**. Note that a name string containing a space in the text must be enclosed in quotes. For example: **"John Smith"**.
System Up Time	See the device's uptime in days, hours, minutes and seconds.
	Telnet to the textual Command Line Interface (CLI) for this device.
	Send email to Enterasys technical support.
	Connect to the Enterasys Web page.

3.3 SWITCH INFORMATION SCREEN

When to Use

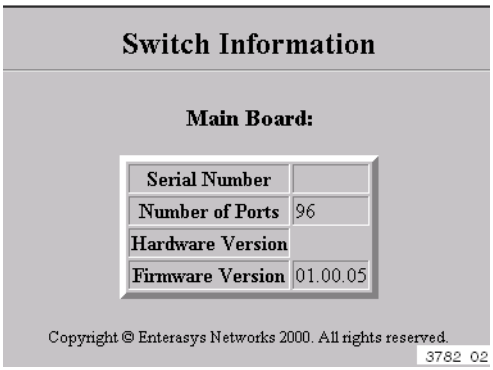
To view information about the main system board, including serial number, number of ports, and hardware and firmware versions.

How to Access

Click on **Switch** on the WebView navigation frame. The Switch Information screen, Figure 3-2, displays.

Screen Example

Figure 3-2 Switch Information Screen



Screen Element Descriptions

Refer to Table 3-2 for a functional description of each screen element.

Table 3-2 Switch Information Screen Element Descriptions

Use this field…	To…
Serial Number	See the serial number of the device's main board.
Number of Ports	See the number of ports available on the device.
Hardware Version	See the device's hardware version number.
Firmware Version	See the device's current firmware version number.

3.4 IP CONFIGURATION SCREEN

When to Use

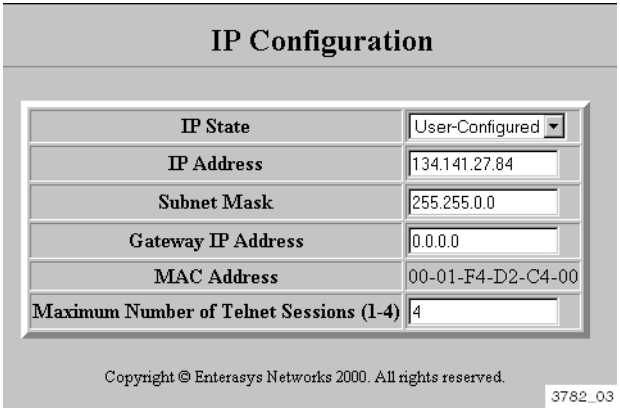
To configure the host IP state, IP address, subnet mask, gateway IP address, and maximum number of Telnet sessions allowed, and to view the device's MAC address.

How to Access

Click on **IP** on the WebView navigation frame. The IP Configuration screen, Figure 3-3, displays.

Screen Example

Figure 3-3 IP Configuration Screen



Screen Element Descriptions

Refer to Table 3-3 for a functional description of each screen element.

Table 3-3 IP Configuration Screen Element Descriptions

Use this field…	To…
IP State	Select the host IP state. Options are: **User-Configured** - IP functionality is enabled based on the default or user-specified IP configuration. (This is the default setting.) **BootP Get IP** - IP is enabled but will not function until a BOOTP (Boot Protocol) reply has been received. BOOTP requests will be periodically broadcast by the device in an effort to learn its IP address. (BOOTP values include the IP address, default gateway, and subnet mask.)
IP Address	See or enter a new local host IP address.
Subnet Mask	See or enter a new local host subnet mask. Default is **255.255.0.0**.
Gateway IP Address	See or enter a new gateway IP address.
MAC Address	See the local host's MAC address.

Table 3-3 IP Configuration Screen Element Descriptions (Continued)

Use this field…	To…
Maximum Number of Telnet Sessions (1-4)	Select the maximum number of Telnet sessions allowed (from **1** to **4**).

3.5 SNMP TRAPS CONFIGURATION SCREEN

When to Use

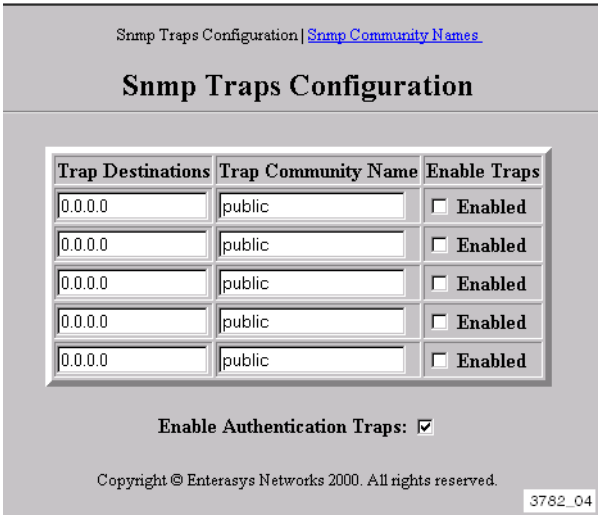
To assign IP addresses where SNMP traps will be sent, to enable or disable traps, and to access the SNMP Community Names screen, where SNMP community names and access policies associated with these traps can be set.

How to Access

Click on **SNMP** on the WebView navigation frame. The SNMP Traps Configuration screen, Figure 3-4, displays.

Screen Example

Figure 3-4 SNMP Traps Configuration Screen



Screen Element Descriptions

Refer to Table 3-4 for a functional description of each screen element.

Table 3-4 SNMP Traps Configuration Screen Element Descriptions

Use this field…	To…
Trap Destinations	Enter a destination IP address for an SNMP trap. This identifies the network management station where SNMP alerts of status changes will be sent.
Trap Community Name	Enter an SNMP community name to associate with the trap. Community names act as passwords to remote SNMP management.
Enable Traps	Enable or disable the SNMP traps associated with the displayed **Trap Destinations** and **Trap Community Name**.
Enable Authentication Traps	Enable the device to issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails.

3.6 SNMP COMMUNITY NAMES SCREEN

When to Use

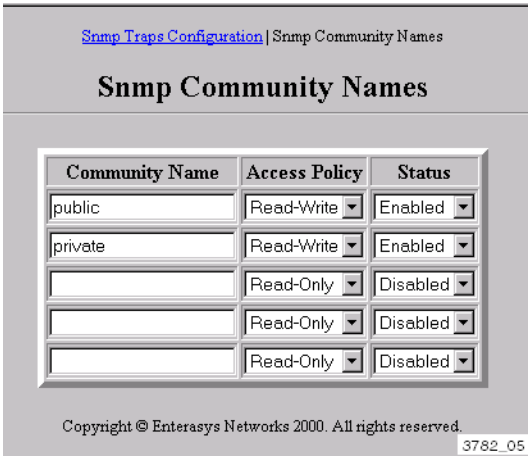
To set SNMP community names and access policies.

How to Access

Click on **SNMP** on the WebView navigation frame. The SNMP Traps Configuration screen, Figure 3-4, displays. Click on **SNMP Community Names** on the content frame. The SNMP Community Names screen, Figure 3-5, displays.

Screen Example

Figure 3-5 SNMP Community Names Screen



Screen Element Descriptions

Refer to Table 3-5 for a functional description of each screen element.

Table 3-5 SNMP Community Names Screen Element Descriptions

Use this field…	To…
Community Name	Enter a community name through which a user will access SNMP management.
Access Policy	Select the access permission accorded each community name. The available access levels are: • **Read-Only**: This community name gives the user read-only access to the device MIB objects, and excludes access to security-protected fields of read-write authorization. • **Read-Write**: This community name gives the user read-write access to the device MIB objects and also gives “super-user” access allowing the user to change all modifiable parameters, including community names, IP addresses, traps and SNMP objects.

Table 3-5 SNMP Community Names Screen Element Descriptions (Continued)

Use this field…	To…
Status	Select the status (**Enabled**, **Disabled** or **Remove**) for each access policy.

3.7 SECURITY CONFIGURATION SCREEN

When to Use

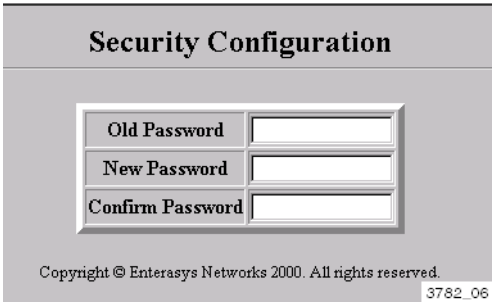
To set a new login password for the device.

How to Access

Click on **Security** on the WebView navigation frame. The Security Configuration screen, Figure 3-6, displays.

Screen Example

Figure 3-6 Security Configuration Screen



Screen Element Descriptions

Refer to Table 3-6 for a functional description of each screen element.

Table 3-6 Security Configuration Screen Element Descriptions

Use this field…	To…
Old Password	Enter the old login password or, if none has been configured on the device, leave this field blank. By default at device start up, no password is configured.
New Password	Enter the new login password.
Confirm Password	Re-enter the new login password.

3.8 TFTP DOWNLOAD MANAGEMENT SCREEN

When to Use

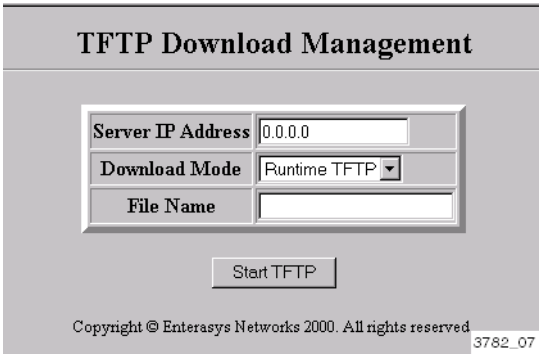
To download a new firmware image from a TFTP server to the device.

How to Access

Click on **Upgrade** on the WebView navigation frame. The TFTP Download Management screen, Figure 3-7, displays.

Screen Example

Figure 3-7 TFTP Download Management Screen



Screen Element Descriptions

Refer to Table 3-7 for a functional description of each screen element.

Table 3-7 TFTP Download Management Screen Element Descriptions

Use this field or button…	To…
Server IP Address	Enter the address of the TFTP server from which the new firmware image file will be downloaded.
Download Mode	Accept the download mode: **Runtime TFTP**.
File Name	Enter the TFTP server path and file name of the new image.
Start TFTP	Start the TFTP download.

3.9 ADDRESS TABLE CONFIGURATION SCREEN

When to Use

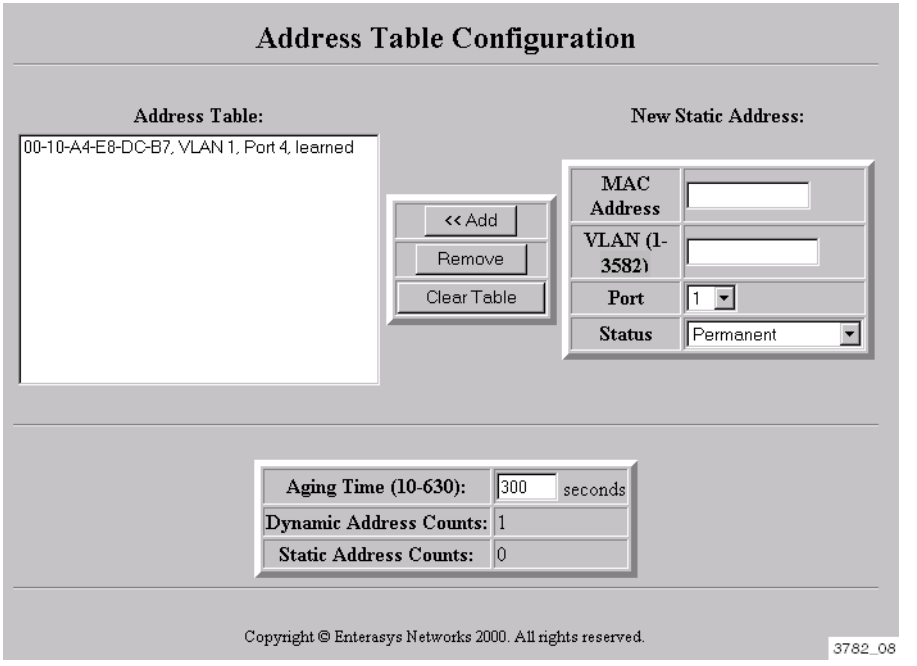
To view entries in the device's address table, add new static address entries, remove entries, and view counts of dynamic and static addresses in the address table.

How to Access

Click on **Address Table** on the WebView navigation frame. The Address Table Configuration screen, Figure 3-8, displays.

Screen Example

Figure 3-8 Address Table Configuration Screen



Screen Element Descriptions

Refer to Table 3-8 for a functional description of each screen element.

Table 3-8 Address Table Configuration Screen Element Descriptions

Use this field or button…	To…
Address Table	See the device's current address table entries.
MAC Address	Enter a MAC address for a new static address table entry.

Table 3-8 Address Table Configuration Screen Element Descriptions (Continued)

Use this field or button…	To…
VLAN (1-3582)	Enter a number (**1** to **3582**) identifying the VLAN to which the MAC address belongs.
Port	Select a port number associated with the MAC Address and VLAN.
Status	Select a status for new static address entries. Valid options are: **Permanent** - Leaves all addresses in the address table, even if the device is reset. **Delete on Reset** - Deletes all new static addresses when the device is reset. **Delete on Timeout** - Deletes all new static addresses when the device times out.
<< Add	Add the new static address entry to the address table.
Remove	Remove a selected entry from the address table. To select an entry, click on it in the **Address Table** field.
Clear Table	Clear all entries in the device's address table.
Aging Time (10-630)	Enter a timeout period (from **10** to **630** seconds) for aging out all dynamically learned MAC addresses and forwarding information.
Dynamic Address Counts	See the number of dynamic addresses in the device's address table.
Static Address Counts	See the number of static addresses in the device's address table. Static addresses are those created by the user using the CLI or the fields in this screen.

3.10 STA INFORMATION SCREEN

When to Use

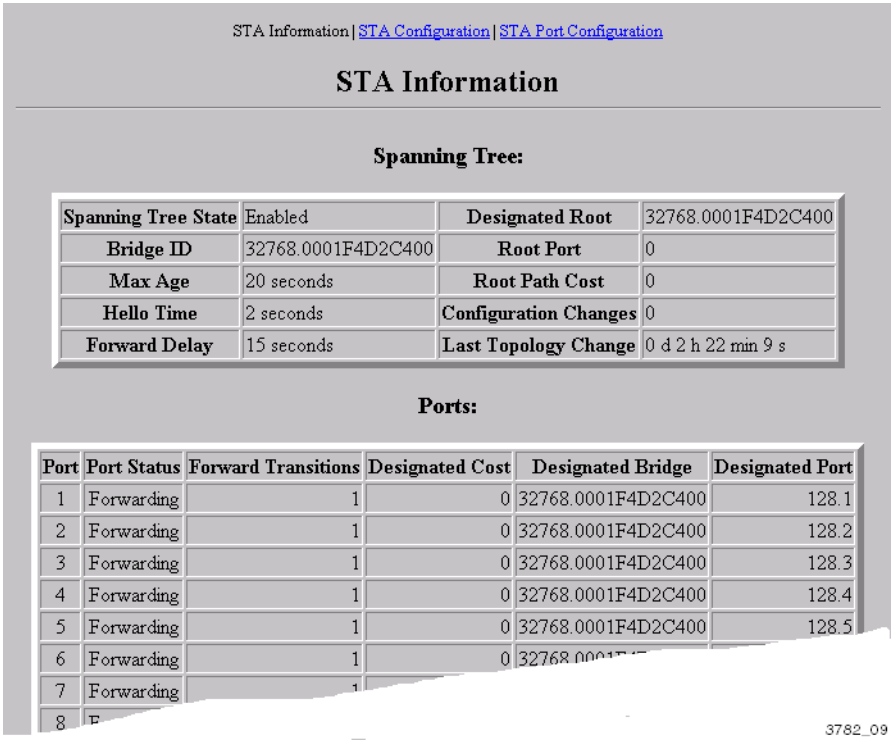
To view Spanning Tree Algorithm (STA) information about the device and about each port, and to access the STA Configuration and STA Port Configuration screens.

How to Access

Click on **STA** on the WebView navigation frame. The STA Information screen, Figure 3-9, displays. Spanning Tree information for the bridge device displays at the top (**Spanning Tree)** portion of the screen. STA information about individual ports displays at the bottom (**Ports**) portion of the screen.

Screen Example

Figure 3-9 STA Information Screen



Screen Element Descriptions

Refer to Table 3-9 for a functional description of each screen element.

Table 3-9 STA Information Screen Element Descriptions

Use this field…	To…
	Spanning Tree:
Spanning Tree State	See whether Spanning Tree is **Enabled** or **Disabled** on the bridge device.
Bridge ID	See a unique identifier for this bridge, consisting of bridge priority plus MAC address (where the address is taken from the switch system).
Max Age	See the maximum number of seconds (**6** to **40**) the bridge device will wait to receive a configuration message before attempting to reconfigure.
Hello Time	See the maximum number of seconds (**1** to **10**) the device waits before sending a bridge hello message (a multicast message indicating the device is active).
Forward Delay	See the maximum number of seconds (**4** to **30**) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames.
Designated Root	See the MAC address of the designated Spanning Tree root bridge. This is the logical center of the Spanning Tree topology.
Root Port	See the port on this device that is closest to the root. This device communicates with the root device through the root port. If no root port is indicated, then this device has been accepted as the root device of the Spanning Tree network.
Root Path Cost	See the path cost from the root port on this device to the root device.
Configuration Changes	See a count of STA configuration changes known to the device.
Last Topology Change	See the time elapsed since the last STA topology change in days, hours, minutes and seconds.
	Ports:
Port	See the port number associated with the displayed Spanning Tree port parameters.

Table 3-9 STA Information Screen Element Descriptions (Continued)

Use this field…	To…
Port Status	See the port's current STA state. Options are: **Disabled** - The port has been disabled by the user or has failed diagnostics. **Blocked** - The port receives STA configuration messages, but does not forward packets. **Listening** - The port will leave blocking state due to topology change, will start transmitting configuration messages, but does not yet forward packets. **Learning** - The port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. The port address table is cleared, and the port begins learning addresses. **Forwarding** - The port forwards packets, and continues learning addresses. The rules defining port status are: • A port on a network segment with no other STA compliant bridging device is always forwarding. • If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked. • All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
Forward Transitions	See counts of the port's forward transitions.
Designated Cost	See the path cost from the transmitting port to the root.
Designated Bridge	See the MAC address of the designated bridge to which the port belongs. This is the switch that is closest to the root switch through which frames will be forwarded to the root.

Table 3-9 STA Information Screen Element Descriptions (Continued)

Use this field…	To…
Designated Port	See the port designation used by STA for forwarding from this port to the root.

3.11 STA CONFIGURATION SCREEN

When to Use

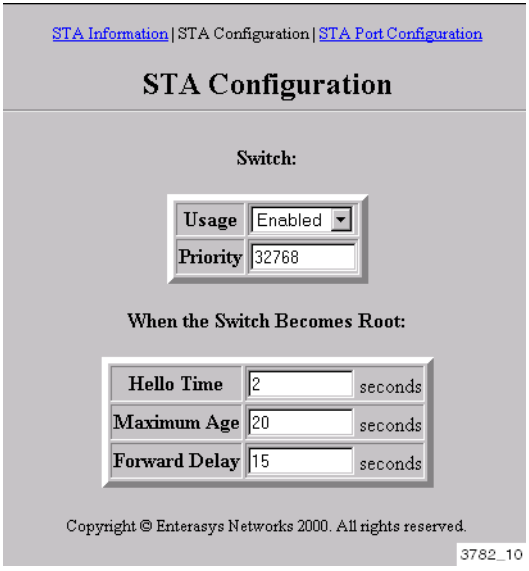
To configure Spanning Tree Algorithm (STA) settings for the device, including parameters for when the device becomes the Spanning Tree root bridge.

How to Access

Click on **STA** on the WebView navigation frame. The STA Information screen, Figure 3-9, displays. Click on **STA Configuration** on the content frame. The STA Configuration screen, Figure 3-10, displays.

Screen Example

Figure 3-10 STA Configuration Screen



Screen Element Descriptions

Refer to Table 3-10 for a functional description of each screen element.

Table 3-10 STA Configuration Screen Element Descriptions

Use this field…	To…
	Switch:
Usage	Select whether Spanning Tree is **Enabled** or **Disabled** on the bridge device.
Priority	Enter the bridge priority for the device. The priority level can be **0** to **65535**, with 65335 being the highest. STA uses device priority to determine the root device, the logical center of the Spanning Tree topology. The device with the highest priority becomes the root.
	When the Switch Becomes Root:
Hello Time	Enter the maximum number of seconds (**1** to **10**) the root device waits before sending a bridge hello message (a multicast message indicating the device is active).
Maximum Age	Enter the maximum number of seconds (**6** to **40**) the root device will wait without receiving a configuration message before attempting to reconfigure.
Forward Delay	Enter the maximum number of seconds (**4** to **30**) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames.

3.12 STA PORT CONFIGURATION SCREEN

When to Use

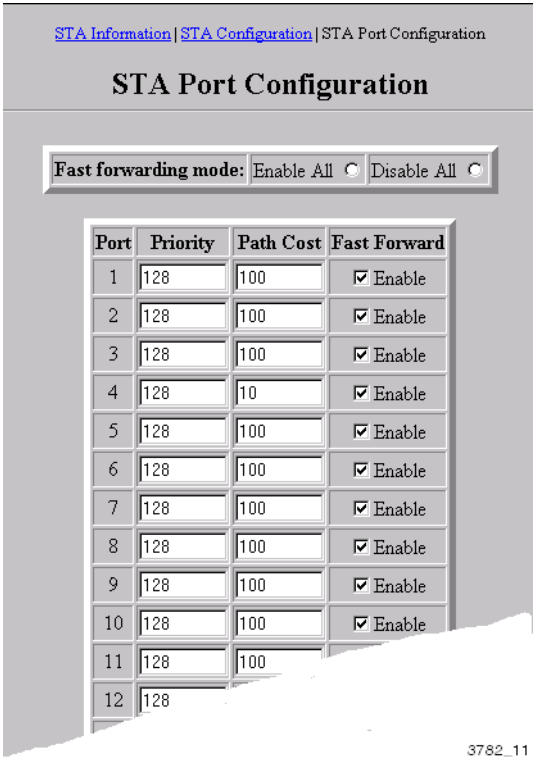
To configure Spanning Tree Algorithm (STA) settings for individual ports on the device.

How to Access

Click on **STA** on the WebView navigation frame. The STA Information screen, Figure 3-9, displays. Click on **STA Port Configuration** on the content frame. The STA Port Configuration screen, Figure 3-11, displays.

Screen Example

Figure 3-11 STA Port Configuration Screen



Screen Element Descriptions

Refer to Table 3-11 for a functional description of each screen element.

Table 3-11 STA Port Configuration Screen Element Descriptions

Use this field…	To…
Fast forwarding mode	Enable or disable fast forwarding mode (also known as STP standby mode) for all ports on the device. This feature causes a Spanning Tree port to enter the forwarding state immediately, bypassing the listening and learning states and allowing for faster network connectivity.
Port	See the port number associated with the displayed Spanning Tree port parameters.

Table 3-11 STA Port Configuration Screen Element Descriptions (Continued)

Use this field…	To…
Priority	Enter a bridge priority value for the port. This number represents the cost of a link in the Spanning Tree bridge. Valid values are from **0** to **128**, with 0 indicating high priority and 128, low priority.
Path Cost	Enter a value (**1** to **65535**) to assign path cost to a port. This setting takes precedence over **Priority**. The parameter entered here is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. The default and recommended cost range is: Ethernet: 100 (50-100) Fast Ethernet: 10 (10-60) Gigabit Ethernet: 1 (1-10)
Fast Forward	Enable or disable fast forwarding mode on individual ports.

3.13 BRIDGE EXTENSION CONFIGURATION SCREEN

When to Use

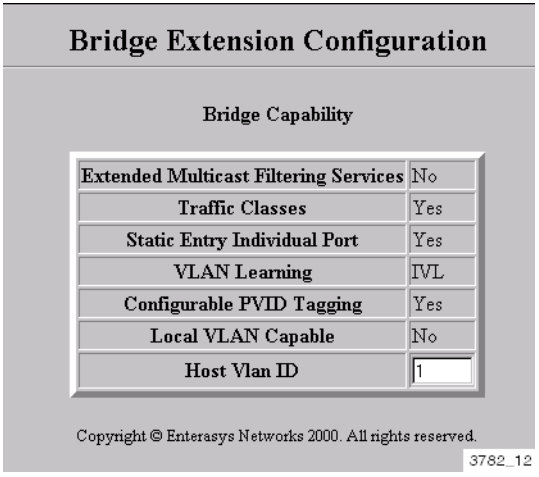
To view bridge MIB extension capabilities configured on the device, and to set the host VLAN ID.

How to Access

Click on **Bridge Extension** on the WebView navigation frame. The Bridge Extension Configuration screen, Figure 3-12, displays.

Screen Example

Figure 3-12 Bridge Extension Configuration Screen



Screen Element Descriptions

Refer to Table 3-12 for a functional description of each screen element.

Table 3-12 Bridge Extension Configuration Screen Element Descriptions

Use this field…	To…
Extended Multicast Filtering Services	See if filtering of individual multicast addresses is active.
Traffic Classes	See if the mapping of user priorities to multiple traffic classes function is active.
Static Entry Individual Port	See if the static filtering for unicast and multicast addresses function is active.
VLAN Learning	See the VLAN learning mode used by the device. **IVL** (Independent VLAN Mode) allows each port to maintain its own VLAN filtering database.

Table 3-12 Bridge Extension Configuration Screen Element Descriptions (Continued)

Use this field…	To…
Configurable PVID Tagging	See if you are allowed to override the default PVID setting (Port VLAN ID used in frame tags) and its egress status (VLAN-tagged or untagged) on each port.
Local VLAN Capable	See if the device supports multiple local bridges (or Spanning Trees).
Host VLAN ID	Enter the number of the VLAN designated as the host VLAN. A host VLAN is a secure VLAN where only designated users are allowed access.

3.14 PORT PRIORITY CONFIGURATION SCREEN

When to Use

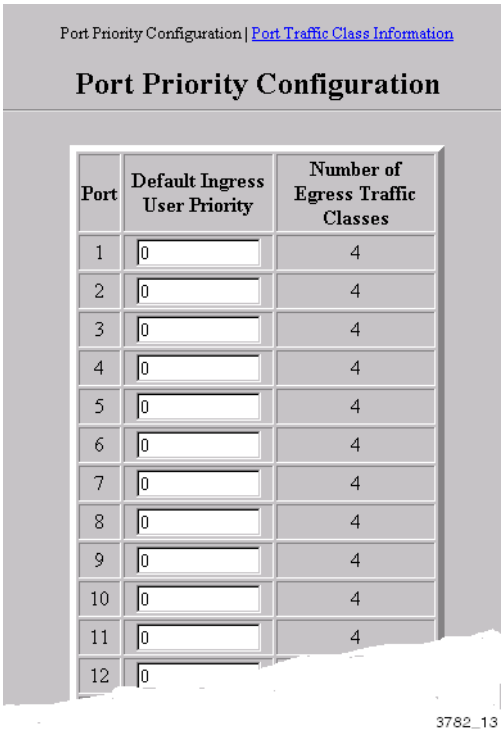
To set the default ingress port priority per port, to view the number of egress traffic classes, or transmit queues, per port, and to access the Port Traffic Class Information screen.

How to Access

Click on **Priority** on the WebView navigation frame. The Port Priority Configuration screen, Figure 3-13, displays.

Screen Example

Figure 3-13 Port Priority Configuration Screen



Screen Element Descriptions

Refer to Table 3-13 for a functional description of each screen element.

Table 3-13 Port Priority Configuration Screen Element Descriptions

Use this field…	To…
Port	See the port number associated with the displayed priority parameters.

Table 3-13 Port Priority Configuration Screen Element Descriptions (Continued)

Use this field…	To…
Default Ingress User Priority	See or enter a new 802.1p port transmit priority for frames that are received (ingress) without priority information in their tag header. Valid priority values are **0** through **7**, with 0 being lowest priority and 7, highest. A port receiving a frame without priority information in its tag header is assigned a priority according to the priority setting on the port. For example, if the priority of a port is set to 5, the frames received through that port without a priority indicated in their tag header are classified as a priority 5. Default port priority is **1**.
Number of Egress Traffic Classes	See the number of egress traffic classes, or transmit queues, available for each port. Of the **4** traffic classes (numbered 0 through 3) available, 0 is assigned the lowest priority queue. Traffic classes can map 802.1p port priorities to transmit queues. For example, if the port priority queue is set to 3 for those frames with a port priority 7, then those frames would be transmitted before any frames contained in traffic classes 2 through 0.

3.15 PORT TRAFFIC CLASS INFORMATION SCREEN

When to Use

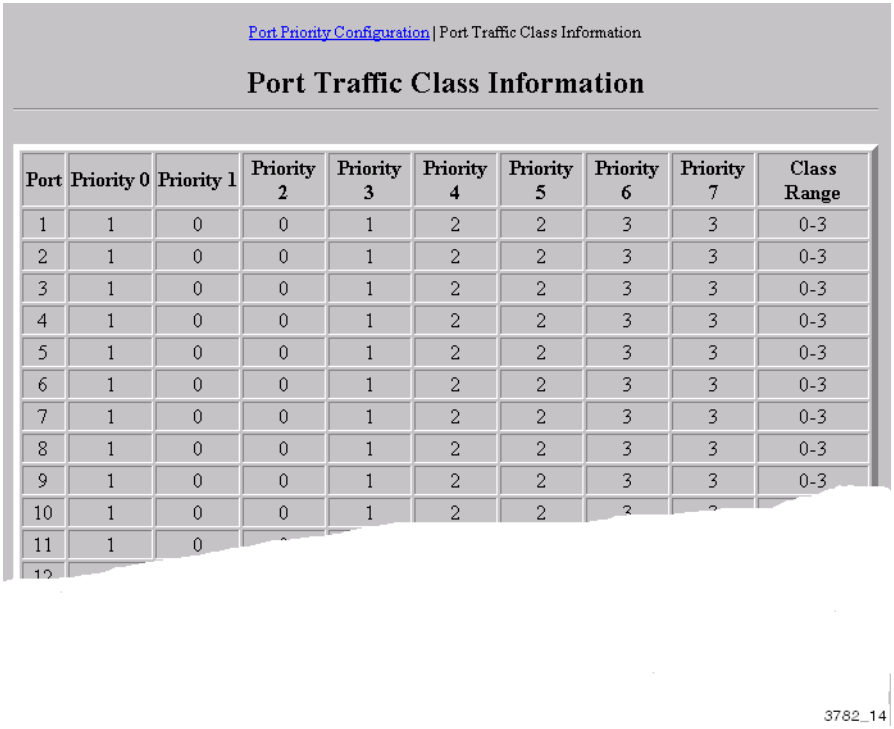
To view port priority-to-transmit queue mapping information.

How to Access

Click on **Priority** on the WebView navigation frame. The Port Priority Configuration screen, Figure 3-13, displays. Click on **Port Traffic Class Information** on the content frame. The Port Traffic Class Information screen, Figure 3-14, displays.

Screen Example

Figure 3-14 Port Traffic Class Information Screen



Screen Element Descriptions

Refer to Table 3-14 for a functional description of each screen element.

Table 3-14 Port Traffic Class Information Screen Element Descriptions

Use this field…	To…
Port	See the port number associated with the displayed priority parameters.

Table 3-14 Port Traffic Class Information Screen Element Descriptions (Continued)

Use this field…	To…
Priority <0 - 7>	See the traffic class, or transmit queue, associated with priority levels 0 through 7 for each port. 0 indicates that the priority has been assigned the lowest transmit queue priority, and 3 indicates it has been assigned the highest. For example, as shown in Figure 3-14, if the port priority queue is set to 3 for frames with a port priority 7, then those frames would be transmitted before any frames contained in traffic classes 2 through 0.
Class Range	See the range of egress traffic classes available for each port. **0-3** indicates there are 4 traffic classes available.

3.16 VLAN BASIC INFORMATION SCREEN

When to Use

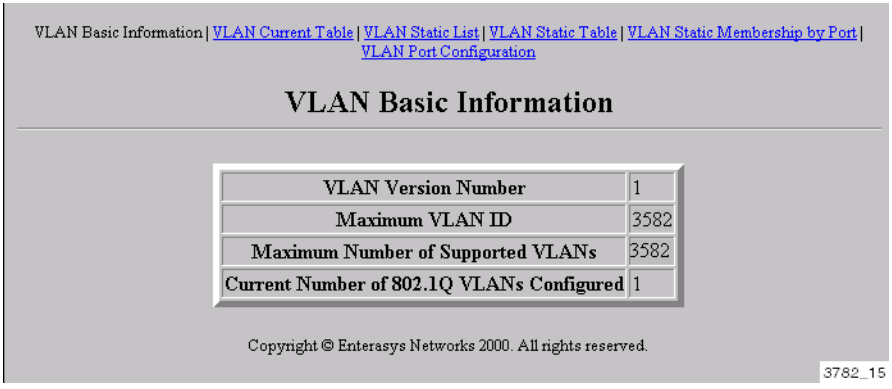
To view basic information about the numbers of VLANs configured on the device, and to access the VLAN Current Table, VLAN Static List, VLAN Static Table, VLAN Static Membership by Port, and VLAN Port Configuration screens.

How to Access

Click on **VLAN** on the WebView navigation frame. The VLAN Basic Information screen, Figure 3-15, displays.

Screen Example

Figure 3-15 VLAN Basic Information Screen



Screen Element Descriptions

Refer to Table 3-15 for a functional description of each screen element.

Table 3-15 VLAN Basic Information Screen Element Descriptions

Use this field…	To…
VLAN Version Number	See the VLAN version used by the device as specified in the IEEE 802.1Q standard.
Maximum VLAN ID	See the maximum number of VLAN IDs that can be recognized by the device.
Maximum Number of Supported VLANs	See the maximum number of VLANs that can be configured on the device.
Current Number of 802.1Q VLANs Configured	See the number of VLANs currently configured on the device.

3.17 VLAN CURRENT TABLE SCREEN

When to Use

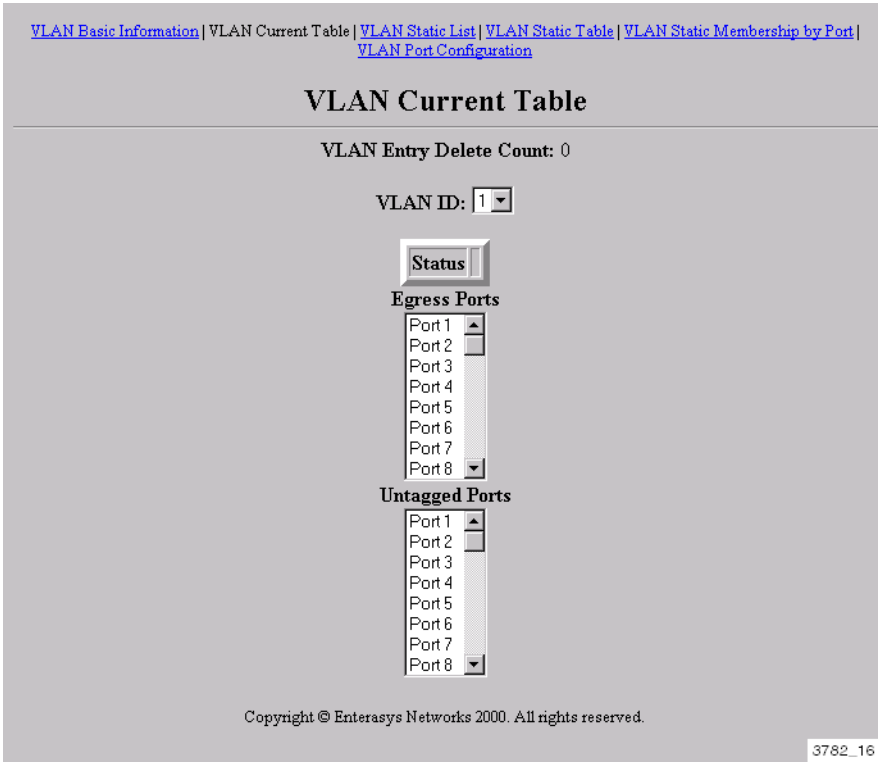
To view information about all static and dynamically created VLANs known to the device, such as which ports belong to a VLAN's egress list and whether or not they are configured to transmit untagged frames.

How to Access

Click on **VLAN** on the WebView navigation frame. The VLAN Basic Information screen, Figure 3-15, displays. Click on **VLAN Current Table** on the content frame. The VLAN Current Table screen, Table 3-16, displays.

Screen Example

Figure 3-16 VLAN Current Table Screen



Screen Element Descriptions

Refer to Table 3-16 for a functional description of each screen element.

Table 3-16 VLAN Current Table Screen Element Descriptions

Use this field…	To…
VLAN Entry Delete Count	See the number of times a VLAN entry has been deleted from this table.
VLAN ID	Select the number identifying the VLAN for which to see port egress information. Default is **1**.

Table 3-16 VLAN Current Table Screen Element Descriptions (Continued)

Use this field…	To…
Egress Ports	See which ports belong to the VLAN's egress list.
Untagged Ports	See which ports belonging to the VLAN are configured to transmit untagged frames.

3.18 VLAN STATIC LIST SCREEN

When to Use

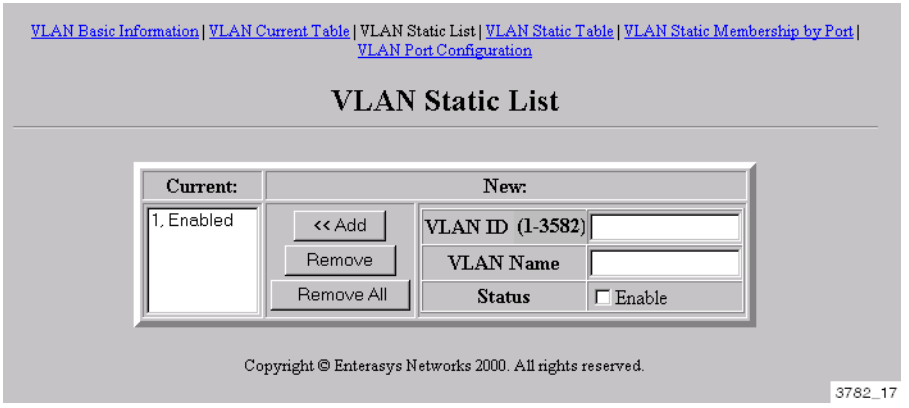
To create new or remove existing static VLANs from the device.

How to Access

Click on **VLAN** on the WebView navigation frame. The VLAN Basic Information screen, Figure 3-15, displays. Click on **VLAN Static List** on the content frame. The VLAN Static List screen, Figure 3-17, displays.

Screen Example

Figure 3-17 VLAN Static List Screen



Screen Element Descriptions

Refer to Table 3-17 for a functional description of each screen element.

Table 3-17 VLAN Static List Screen Element Descriptions

Use this field or button…	To…
Current	See the ID number(s) for currently configured VLANs and whether or not they are enabled or disabled.
VLAN ID (1-3582)	Enter a unique number (**1** to **3582**) for the new VLAN to be created.
VLAN Name	Enter a name (1 to 32 characters) for the new or previously created static VLAN.
Status	**Enable** or **Disable** the static VLAN.
<< Add	Add the new static VLAN to the list of those recognized by the device.
Remove	Remove a selected entry from the device's VLAN list. To select an entry click on it in the **Current** field.
Remove All	Remove all entries from the device's VLAN list.

3.19 VLAN STATIC TABLE SCREEN

When to Use

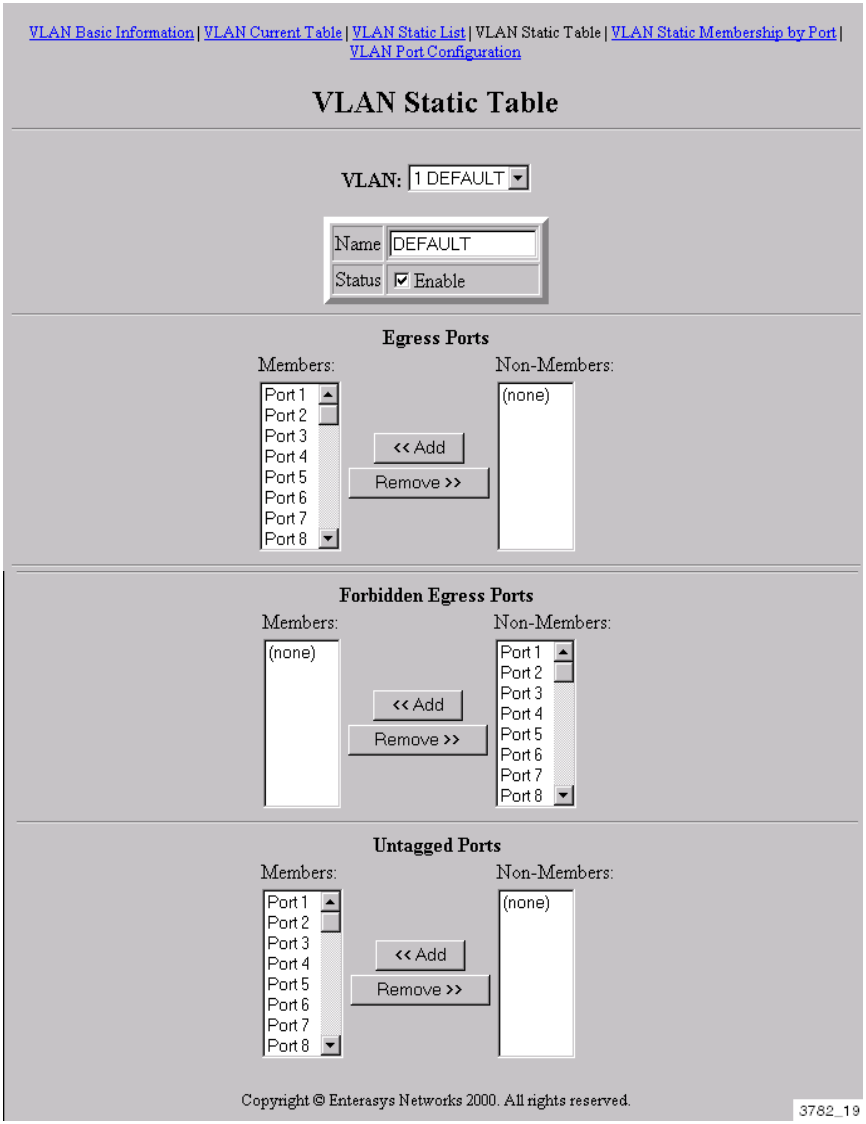
To configure a static VLAN's egress list, including which ports belong to the list, which ports can transmit untagged frames, and which are forbidden ports.

How to Access

Click on **VLAN** on the WebView navigation frame. The VLAN Basic Information screen, Figure 3-15, displays. Click on **VLAN Static Table** on the content frame. The VLAN Static Table screen, Figure 3-18, displays.

Screen Example

Figure 3-18 VLAN Static Table Screen



Screen Element Descriptions

Refer to Table 3-18 for a functional description of each screen element.

Table 3-18 VLAN Static Table Screen Element Descriptions

Use this field or button…	To…
VLAN	Select the VLAN ID and name for which to configure VLAN parameters.
Name	See the VLAN name.
Status	**Enable** or disable the static VLAN.
	Egress Ports
Members	See which ports belong to the static VLAN's egress list.
Non-Members	See which ports do not belong to the static VLAN's egress list.
<< Add	Make a selected **Non-Member** port part of the **Member** egress list for the static VLAN.
Remove >>	Make a selected **Member** port part of the **Non-Member** egress list for the static VLAN.
	Forbidden Egress Ports
Members	See which ports belong to the static VLAN's forbidden egress list. Frames containing a forbidden VLAN tag will be prevented from egressing from the specified port.
Non-Members	See which ports do not belong to the static VLAN's forbidden egress list.
<< Add	Make a selected **Non-Member** port part of the **Member** list of forbidden ports for the static VLAN.
Remove >>	Make a selected **Member** port part of the **Non-Member** egress list of forbidden ports for the static VLAN.

Table 3-18 VLAN Static Table Screen Element Descriptions (Continued)

Use this field or button…	To…
	Untagged Ports
Members	See which ports are configured to transmit untagged frames for a static VLAN.
Non-Members	See which ports are not configured to transmit untagged frames for a static VLAN.
<< Add	Make a selected **Non-Member** port part of the **Member** list of ports able to transmit untagged frames for the static VLAN.
Remove >>	Make a selected **Member** port part of the **Non-Member** egress list of ports not able to transmit untagged frames for the static VLAN.

3.20 VLAN STATIC MEMBERSHIP BY PORT SCREEN

When to Use

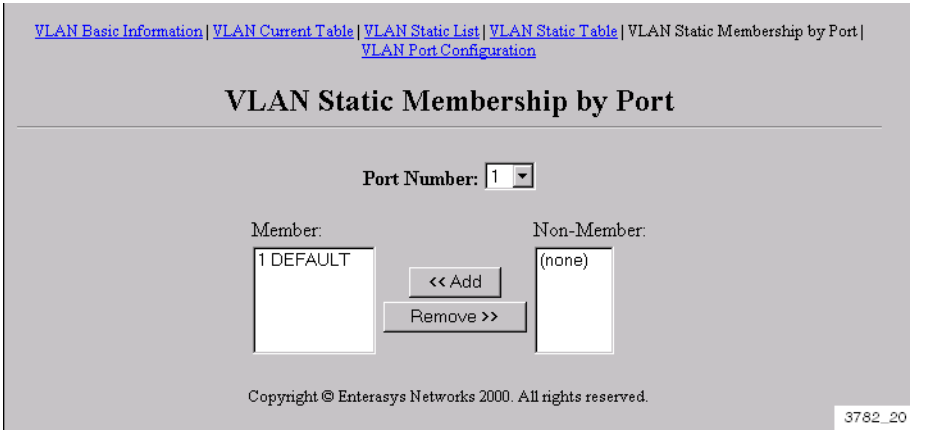
To add ports to or remove ports from a static VLAN. Static VLANs are those created by the user using the CLI or the fields in the VLAN configuration screens.

How to Access

Click on **VLAN** on the WebView navigation frame. The VLAN Basic Information screen, Figure 3-15, displays. Click on **VLAN Static Membership by Port** on the content frame. The VLAN Static Membership by Port screen, Figure 3-19, displays.

Screen Example

Figure 3-19 VLAN Static Membership by Port Screen



Screen Element Descriptions

Refer to Table 3-19 for a functional description of each screen element.

Table 3-19 VLAN Static Membership by Port Screen Element Descriptions

Use this field or button…	To…
Port Number	Select the number of the port for which to configure VLAN membership.
Member	See the number and name of the VLAN of which the port is a member.
Non-Member	See the number and name of the VLAN of which the port is not a member.
<< Add	Make the port a **Member** of the selected static VLAN.
Remove >>	Make the port a **Non-Member** of the selected static VLAN.

3.21 VLAN PORT CONFIGURATION SCREEN

When to Use

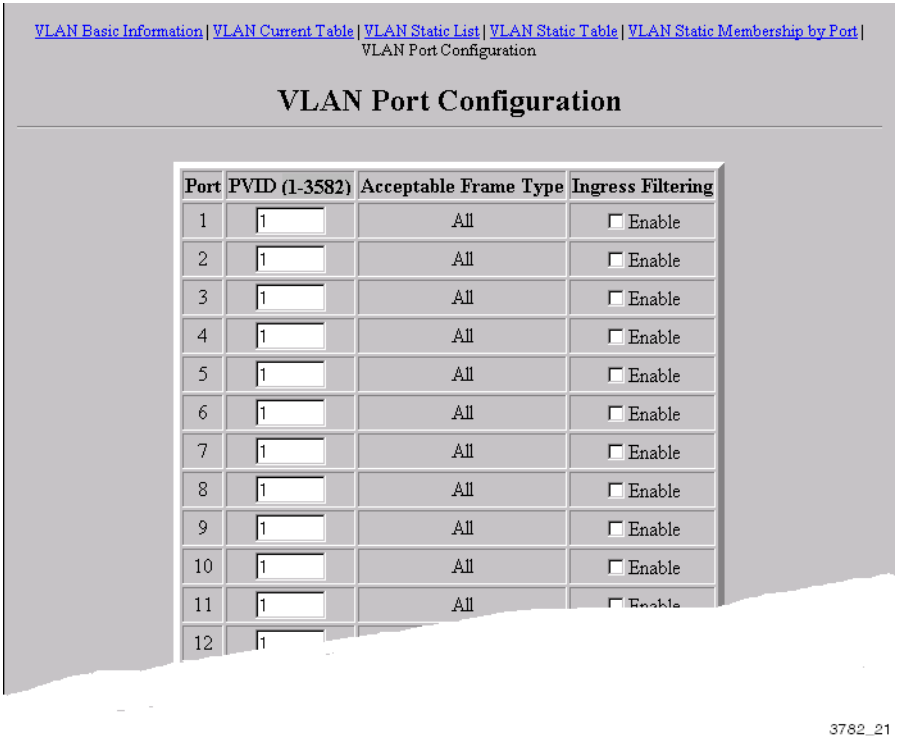
To assign default VLAN IDs to untagged frames, and to enable or disable ingress filtering on one or more ports.

How to Access

Click on **VLAN** on the WebView navigation frame. The VLAN Basic Information screen, Figure 3-15, displays. Click on **VLAN Port Configuration** on the content frame. The VLAN Configuration screen, Figure 3-20, displays.

Screen Example

Figure 3-20 VLAN Port Configuration Screen



Screen Element Descriptions

Refer to Table 3-20 for a functional description of each screen element.

Table 3-20 VLAN Port Configuration Screen Element Descriptions

Use this field…	To…
Port	See the number of the port for which to configure default VLAN ID and ingress filtering status.
PVID (1-3582)	Enter a Port VLAN ID (**1** to **3582**). Untagged frames received on the port will be assigned this VLAN number. By default, all ports are members of VLAN ID 1, the default VLAN.
Acceptable Frame Type	See the acceptable frame type (i.e., RIP) the port is configured to transmit.
Ingress Filtering	Enable or disable ingress filtering on the port. This limits incoming frames according to the port VLAN egress list. If the port is not on the VLAN egress list of the VLAN ID indicated in the incoming frame, then the frame is dropped and not forwarded.

3.22 IGMP CONFIGURATION SCREEN

When to Use

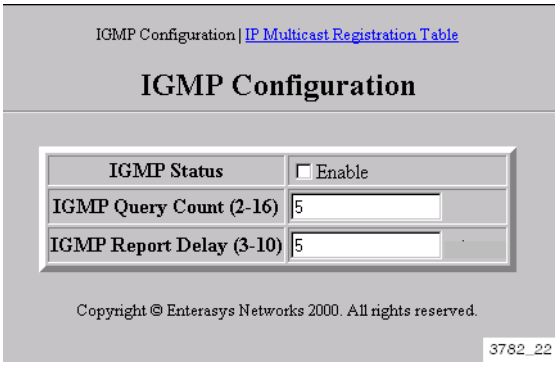
To enable IGMP (Internet Group Management Protocol) on the device, to configure IGMP parameters, and to access the IP Multicast Registration Table screen.

How to Access

Click on **IGMP** on the WebView navigation frame. The IGMP Configuration screen, Figure 3-21, displays.

Screen Example

Figure 3-21 IGMP Configuration Screen



Screen Element Descriptions

Refer to Table 3-21 for a functional description of each screen element.

Table 3-21 IGMP Configuration Screen Element Descriptions

Use this field…	To…
IGMP Status	Enable or disable IGMP snooping on the device. This allows a host to inform the device it wants to receive transmissions addressed to a specific multicast group.
IGMP Query Count (2-16)	Enter the time in minutes (**2** to **16**) for the device to continue sending IGMP queries before removing a port from an IGMP group.
IGMP Report Delay (3-10)	Enter the number of queries (**3** to **10**) that must be missed before an IGMP report delay timer is started.

3.23 IP MULTICAST REGISTRATION TABLE SCREEN

When to Use

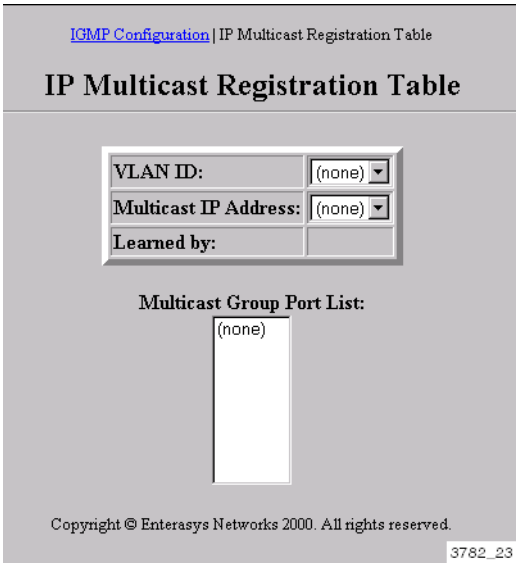
To view the status of IGMP groups on the device. This includes the VLAN port configured to transmit IGMP multicast transmissions, its VLAN ID, and the IP addresses of the ports asking to receive those transmissions as part of the IGMP group.

How to Access

Click on **IGMP** on the WebView navigation frame. The IGMP Configuration screen, Figure 3-21, displays. Click on **IP Multicast Registration Table** on the content frame. The IP Multicast Registration Table screen, Figure 3-22, displays.

Screen Example

Figure 3-22 IP Multicast Registration Table Screen



Screen Element Descriptions

Refer to Table 3-22 for a functional description of each screen element.

Table 3-22 IP Multicast Registration Table Screen Element Descriptions

Use this field…	To…
VLAN ID	Select the identifying number of the VLAN configured for IGMP.
Multicast IP Address	Select the IP address associated with the VLAN ID through which all multicast traffic is forwarded.
Learned by:	See the manner in which the address was learned (Dynamic or IGMP).

Table 3-22 IP Multicast Registration Table Screen Element Descriptions (Continued)

Use this field…	To…
Multicast Group Port List	See the port(s) within this VLAN that wish to receive multicast transmissions.

3.24 PORT INFORMATION SCREEN

When to Use

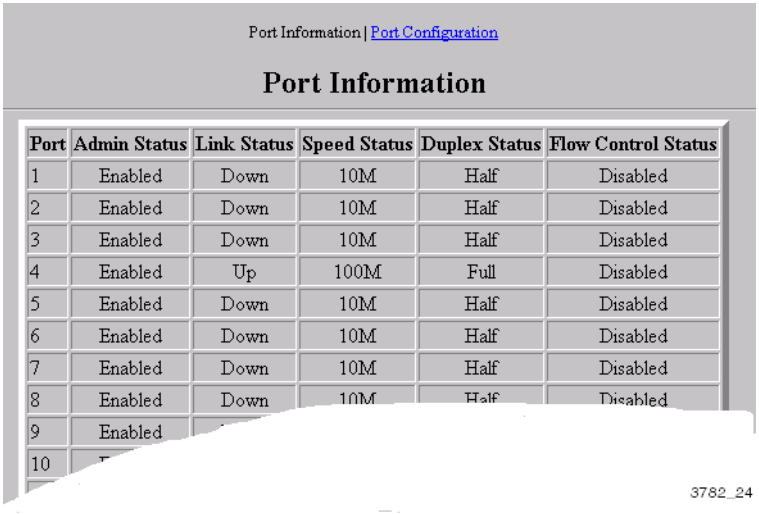
To view port administrative, link, speed, duplex and flow control status, and to access the Port Configuration screen.

How to Access

Click on **Port** on the WebView navigation frame. The Port Information screen, Figure 3-23, displays.

Screen Example

Figure 3-23 Port Information Screen



Screen Element Descriptions

Refer to Table 3-23 for a functional description of each screen element.

Table 3-23 Port Information Screen Element Descriptions

Use this field…	To…
Port	See the port number associated with the displayed status information.
Admin Status	See whether the port is **Enabled** (up) or **Disabled** (down).
Link Status	See whether the port has a valid link (**Up** or **Down**). Link status will be down until a link is established to an external device and the port is enabled.
Speed Status	See the port's operational speed in Mbps (**10M**, **100M** or **1000M**).
Duplex Status	See the port's duplex mode. Options are: **10M Half-Duplex**, **10M Full-Duplex**, **100M Half-Duplex**, **100M Full-Duplex**, and **Auto-Negotiation**.
Flow Control Status	See the port's flow control status (**Enabled** or **Disabled**). Flow control is used to manage the transmission between two devices as specified by IEEE 802.3x to prevent receiving ports from being overwhelmed by frames from transmitting devices.

3.25 PORT CONFIGURATION SCREEN

When to Use

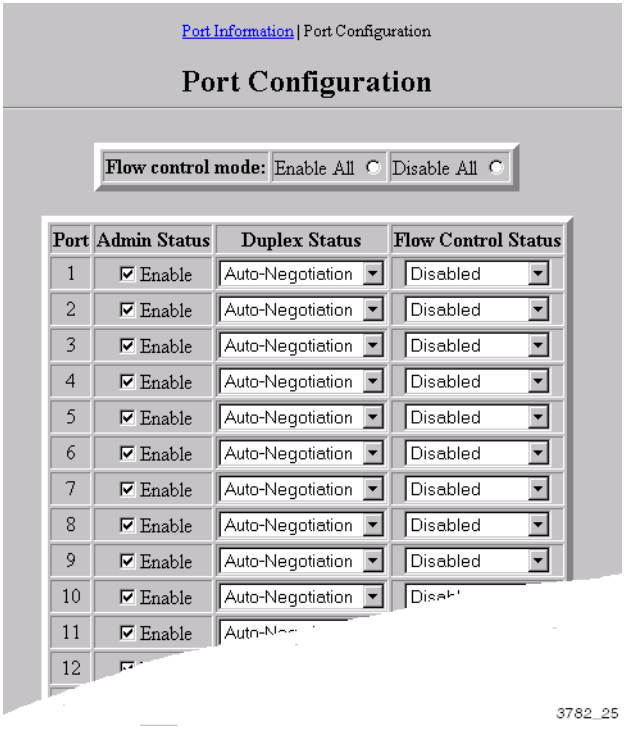
To set port flow control, administrative, and duplex status.

How to Access

Click on **Port** on the WebView navigation frame. The Port Information screen, Figure 3-23, displays. Click on **Port Configuration** on the content frame. The Port Configuration screen, Figure 3-24, displays.

Screen Example

Figure 3-24 Port Configuration Screen



Screen Element Descriptions

Refer to Table 3-24 for a functional description of each screen element.

Table 3-24 Port Configuration Screen Element Descriptions

Use this field…	To…
Flow control mode	**Enable All** or **Disable All** ports for flow control mode.
Port	See the port number associated with the displayed status information.
Admin Status	**Enable** or disable the port.

Table 3-24 Port Configuration Screen Element Descriptions (Continued)

Use this field…	To…
Duplex Status	Set the port's duplex mode. Options are: **10M Half-Duplex**, **10M Full-Duplex**, **100M Half-Duplex**, **100M Full-Duplex**, and **Auto-Negotiation**.
Flow Control Status	Set the port's flow control status (**Enabled** or **Disabled**). Flow control is used to manage the transmission between two devices as specified by IEEE 802.3x to prevent receiving ports from being overwhelmed by frames from transmitting devices.

3.26 MIRROR PORT CONFIGURATION SCREEN

When to Use

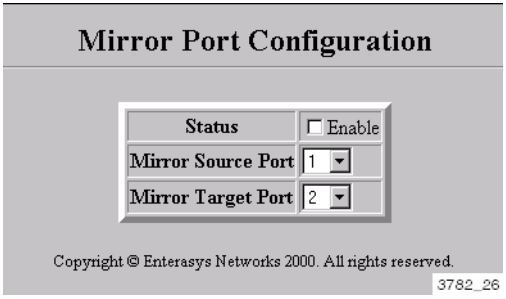
To enable port mirroring and to set a source and target port for mirroring. The Matrix E1 allows you to mirror the traffic being switched on a port for the purposes of network traffic analysis and connection assurance. When port mirroring is enabled, the target port becomes a monitor port for the source port within the device.

How to Access

Click on **Mirror** on the WebView navigation frame. The Mirror Port Configuration screen, Figure 3-25, displays.

Screen Example

Figure 3-25 Mirror Port Configuration Screen



Screen Element Descriptions

Refer to Table 3-25 for a functional description of each screen element.

Table 3-25 Mirror Port Configuration Screen Element Descriptions

Use this field…	To…
Status	Enable port mirroring between the selected **Source Port** and **Target Port**.
Mirror Source Port	Select a source port on which the traffic will be monitored.
Mirror Target Port	Select a target port that will duplicate or “mirror” all the traffic on the monitored source port.

3.27 PORT TRUNKING CONFIGURATION SCREEN

When to Use

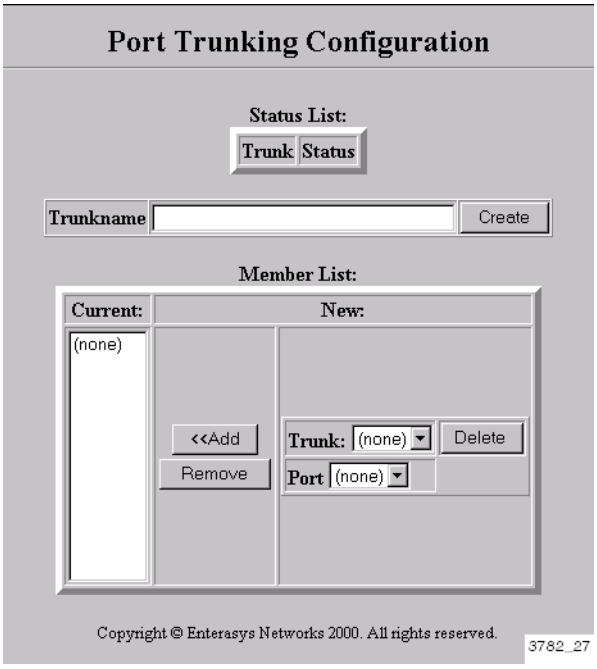
To add or remove trunks on the device, and to add or remove trunk ports from existing trunks.

How to Access

Click on **Trunk** on the WebView navigation frame. The Port Trunking Configuration screen, Figure 3-26, displays.

Screen Example

Figure 3-26 Port Trunking Configuration Screen



Screen Element Descriptions

Refer to Table 3-26 for a functional description of each screen element.

Table 3-26 Port Trunking Configuration Screen Element Descriptions

Use this field or button…	To…
	Status List:
Trunkname	Enter a name for the trunk to be created.
Create	Create a new trunk with the name specified.

Table 3-26 Port Trunking Configuration Screen Element Descriptions (Continued)

Use this field or button…	To…
	Member List:
Current	See a list of trunks and member ports currently configured on the device.
Trunk	Select a trunk name to which to **Add** member ports, or to **Delete** from the device.
Port	Select a member port to add to the specified trunk.
<< Add	Add the specified **Port** to the specified **Trunk Member List**.
Remove	Remove the specified **Port** from the specified **Trunk Member List**.
Delete	Delete the specified trunk from the device.

3.28 PORT STATISTICS SCREEN

When to Use

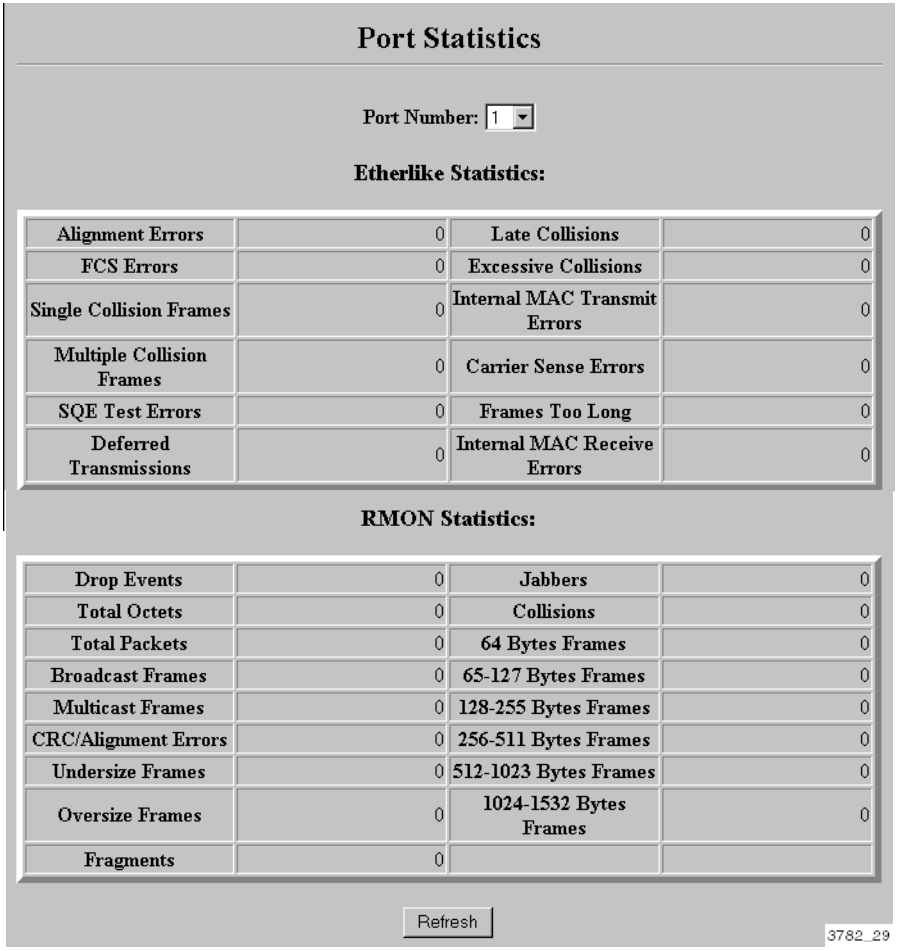
To view port Ethernet-like MIB statistics and RMON statistics.

How to Access

Click on **Statistics** on the WebView navigation frame. The Port Statistics screen, Figure 3-27 displays.

Screen Example

Figure 3-27 Port Statistics Screen



Screen Element Descriptions

Refer to Table 3-27 for a functional description of each screen element.

Table 3-27 Port Statistics Screen Element Descriptions

Use this field or button…	To…
Port Number	Select the number of the port for which to view statistics.
	Etherlike Statistics
Alignment Errors	For 10 Mbps ports, see counts of alignment errors (mis-synchronized data packets). For 100 Mbps ports, see counts of the sum of alignment errors and code errors (frames received with rxerror signal).
FCS Errors	See the number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames	See the number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	See a count of successfully transmitted frames for which transmission is inhibited by more that one collision.
SQE Test Errors	See a count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions	See a count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	See the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions	See the number of frames for which transmission failed due to excessive collisions.
Internal MAC Transmit Errors	See the number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors	See the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	See the number of frames received that exceed the maximum permitted frame size.
Internal MAC Receive Errors	See the number of frames for which reception failed due to an internal MAC sublayer receive error.

Table 3-27 Port Statistics Screen Element Descriptions (Continued)

Use this field or button…	To…
	RMON Statistics:
Drop Events	See the total number of times that the RMON agent was forced to discard frames due to lack of available switch resources. This does not display the number of frames dropped, only the number of times the RMON agent was forced to discard frames.
Total Octets	See the total number of octets (bytes) of data, including those in bad frames, received on this interface.
Total Packets	See the total number of packets (including bad frames, broadcast frames, and multicast frames) received on this interface.
Broadcast Frames	See the total number of good frames that were directed to the broadcast address. This value does not include multicast frames.
Muticast Frames	See the total number of good frames that were directed to the multicast address. This value does not include broadcast frames.
CRC/Alignment Errors	See the number of frames with bad Cyclic Redundancy Checks (CRC) received from the network. The CRC is a 4-byte field in the data frame that ensures that the data received is the same as the data that was originally sent.
Undersize Frames	See the number of frames received containing less than the minimum Ethernet frame size of 64 bytes (not including the preamble) but having a valid CRC.
Oversize Frames	See the number of frames received that exceeded 1516 data bytes (not including the preamble) but had a valid CRC.
Fragments	See the number of received frames that are not the minimum number of bytes in length, or received frames that had a bad or missing Frame Check Sequence (FCS), were less than 64 bytes in length (excluding framing bits, but including FCS bytes) and had an invalid CRC. It is normal for this value to increment since fragments are a normal result of collisions in a half-duplex network.

Table 3-27 Port Statistics Screen Element Descriptions (Continued)

Use this field or button…	To…
Jabbers	See the total number of frames that were greater than 1518 bytes and had either a bad FCS or a bad CRC.
Collisions	See the total number of collisions that have occurred on this interface.
64 Bytes Frames	See the total number of frames, including bad frames, received that were 64 bytes in length (excluding framing bits, but including FCS bytes).
65 – 127 Bytes Frames	See the total number of frames, including bad frames, received that were between 65 and 127 bytes in length (excluding framing bits, but including FCS bytes).
128 – 255 Bytes Frames	See the total number of frames, including bad frames, received that were between 128 and 255 bytes in length (excluding framing bits, but including FCS bytes).
256 – 511 Bytes Frames	See the total number of frames, including bad frames, received that were between 256 and 511 bytes in length (excluding framing bits, but including FCS bytes).
512 – 1023 Bytes Frames	See the total number of frames, including bad frames, received that were between 512 and 1023 bytes in length (excluding framing bits, but including FCS bytes).
1024 – 1532 Bytes Frames	See the total number of frames, including bad frames, received that were between 1024 and 1532 bytes in length (excluding framing bits, but including FCS bytes).
Refresh	Refresh the Port Statistics screen.

3.29 CONSOLE CONFIGURATION SCREEN

When to Use

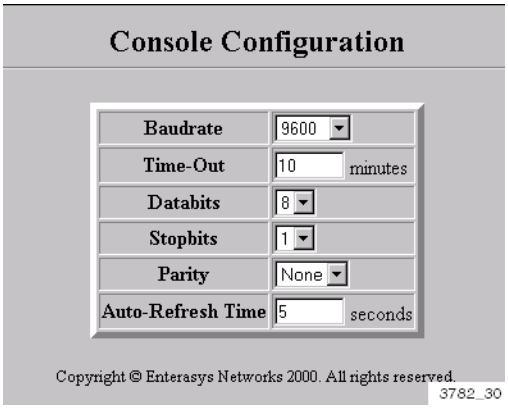
To configure device console settings, such as baud rate, time out, and auto refresh rate.

How to Access

Click on **Console** on the WebView navigation frame. The Console Configuration screen, Figure 3-28, displays.

Screen Example

Figure 3-28 Console Configuration Screen



Screen Element Descriptions

Refer to Table 3-28 for a functional description of each screen element.

Table 3-28 Console Configuration Screen Element Descriptions

Use this field…	To…
Baudrate	Select the console baud rate.
Time-Out	Enter the time in minutes that must elapse before the device times out.
Databits	Select the console's databits.
Stopbits	Select the console's stopbits.
Parity	Select the parity type.
Auto-Refresh Time	Enter the time in seconds that must elapse before the device console auto refreshes.